Federal Computer Incident Response Center

The FedCIRC Bits & Bytes

A monthly newsletter for Information System Security Managers/Officers & System Administrators

June 1, 2001 Volume II, Issue 5

A Note from the Director

We are living in a world in which everything is accessible at the click of a mouse button. We have become habitual net surfers, but the dangers of being a netizen are rarely a consideration as we click our way from site to site. We trust in the systems and assume they offer protection for our sensitive information and that what we see is truly what we get. Naively, we bathe in that false sense of security, unaware of threats that live in the shadows along the information super highway. Well, wake up and smell the cyber-coffee, my friend. The vast uncharted territories of the global Internet harbor horrors that would make anyone cower in fear. Hackers, foreign agents, thieves and good people all live together in the cyber-world but the poor “good guy” is too often unaware of the presence of those evil doers. To top it all off, the bug of bugs, the computer virus, rips across the Internet, exploiting system weaknesses, advanced capabilities of legitimate software applications and the innocent user.

We have to change the way we operate our networks. User training is too often focused on very basic security issues or the use of a variety of applications. In the typical user awareness training, the specifics of email attachments and their ability to hide malicious code or masquerade as a legitimate document or graphic file are not sufficiently addressed. We cannot blame the user for virus proliferation if we throw them into an automated environment without first explaining a few operating system basics. Certain file types can harbor executable content. The intent of this file capability was good. It gave tremendous power to people performing business functions and developing “smart documents.” These documents could modify themselves according to rule sets established by the originator. However, those same capabilities could be harnessed by someone with less than good intentions to unleash catastrophic effects. Embedded document macros or scripts could not only be used as work enhancement tools but also could be turned into a weapon with no specific target in mind. Certainly the adage we hear in every security forum rings true…..”Security is everyone’s responsibility” but it is unrealistic to hold someone responsible for being security conscious when a security baseline has not been adequately established. When possible, the awareness training effort should convey appropriate security information before it becomes an issue. Even the least technical user can understand some of the important basics. Perhaps it is time to review your awareness topics and include some information about attachment content before your training initiatives become damage control efforts. Today’s computer virus is becoming more intelligent. We need to ensure our users keep pace. Technology cannot completely fill the void.

One additional note, Larry Hale has joined the FedCIRC team as our Liaison Director. Larry has a broad background in cyber incident response and critical infrastructure protection. He has previously served as Chief of the Watch and Warning Unit at the National Infrastructure Protection Center and was a member of the Pentagon's Joint Staff Information Operations Response Cell, which preceded the founding of the Joint Task Force for Computer Network Operations.

Larry will be working to raise the awareness of Information Systems security among the Federal agencies, and to inform our customers of the value and services that FedCIRC provides.

Who is Responsible for Virus Outbreaks?

In the last several years, the number of viruses developed has become astounding. With the growth of the Internet these virus outbreaks are moving faster than ever. Virus developers have become more cunning, and their methods continually attempt to overcome the anti-virus solutions. In general, they claim they “never intended to harm the people... but after all, it’s their own fault they got infected with the virus”, or so said the 20 year-old creator of the Kournikova bug.

Computer viruses have the ability to infect your system and destroy programs, data and even hardware. There are several categories of viruses such as Executable, Boot-sector, Partition-table, Memory-resident, and Macro viruses. Over half of the virus incidents reported are caused by macro viruses which infect various system platforms and programs.

We cannot rely on just one tool alone. We need to keep our anti-virus programs current with the latest virus signatures. The assumption that firewalls and other tools will defend against malicious code is naive and dangerous! Malicious code writers are not only developing virus code, but also software to write this code. This places virus creation tools in the hands of everyone. As tools become more sophisticated, multi-layered technologies and procedures are needed to thwart malicious code.

Personal Infrastructure Protection 101:
What To Do If You Lose Your Purse or Wallet

Critical Infrastructure Protection is a top priority for our Nation’s Government and Industry. However, let’s take infrastructure protection to a personal level. Let's talk about what you should do if you lose your purse or wallet. The following are three basic but very important steps you should take to protect your bank/credit card accounts and credit status.

1. Cancel your credit cards immediately! Key Information about bank/credit card numbers and reporting information should be stored in a safe place for ready retrieval.

2. File a police report immediately in the jurisdiction where your personal property was lost or stolen. This proves to credit providers you were diligent, and is a first step toward an investigation.

3. **MOST IMPORTANT** - Report the loss to the three national credit, reporting organizations immediately to place a “fraud alert” on your name and Social Security Number. The “fraud alert” means any company that checks your credit knows your information was stolen and they have to contact you by phone to authorize new credit.

a. Equifax 1-800 525-6285

b. Experian (formerly TRW) 1-800-301-7195

c. Trans Union 1-800-680-7289

d. Social Security Administration also has a fraud line at 1-800-269-0271

Statistics

Current statistics indicate a substantial increase in the number of reported incidents. Since January 1st of this year, 471 reports have been received compared to 586 for the entire previous year. Of more importance is the increase in the number of root compromises. Of the 471 reported incidents this calendar year, 142 have resulted in root compromise in contrast to 155 for year 2000. As hackers continue to develop scripts to automate the explotation of known vulnerabilities, the number of unauthorized intrusions are growing and the skill level to exploit vulnerabilities is decreasing. This trend supports the rising statistics for the number of intrusions reported and gives credence to expectations of futher increases in the future.

Calendar of Events

Network Intrusion Detection
Dates: June 11-13, Aug 13-15, or Nov 12-14, 2001
Locations: varies
POC: MIS Training Institute
508-879-7999
http://www.misti.com/seminar_list.asp

Managing Risks to Information Assets
Date: June 19-21, Aug 28-30 or Oct. 9-11, 2001
Location: Pittsburgh, PA
POC: Carnegie Mellon Univ, Software Engineering Institute (CERT/CC)
412-268-7702
http://www.cert.org/nav/training.html#infassets

Seminar on Internet and Web Security and The Good Guys' Guide to Network Vulnerability Testing
Date: June 25, 2001
Location: Gaithersburg, MD
POC: National Institute of Standards and Technology
301-975-3883
http://www.nist.gov/conferences

Performing a Security Forensics Review
Date: July 12-13 or Nov 19-20, 2001
Location: varies
POC: MIS Training Institute
508-879-7999
http://www.misti.com/seminar_list.asp

WebSec 2001: The E-Security Conference and Expo
Date: August 4-9, 2001
Location: Anaheim, CA
POC: MIS Training Institute
508-879-7999
http://www.misti.com/conference_show.asp

Latest FedCIRC Advisories

FedCIRC Advisory FA-2001-09
Superfluous Decoding Vulnerability in IIS

FedCIRC Advisory FA-2001-10
sadmind/IIS Worm

FedCIRC Advisory FA-2001-11
Buffer Overflow Vulnerability in MicroSoft IIS 5.0

FedCIRC Advisory FA-2001-12
Statistical Weakness in TCP/IP Initial Sequence Numbers

The FedCIRC Bits & Bytes Newsletter

Technical Director
David Jarrell
Liaison Director
Lawrence Hale
Operations Liaison
Connie Oden
Editor
Corliss A. McCain
Contributing Editors
David Adler
Kenneth Grossman
Michael C. Smith
Corliss A. McCain

We welcome your input! To submit your related articles and notices for future issues, please contact FedCIRC at 202-708-5060. Deadline for submissions is the 15th of each month. Articles may be edited for length and content. Back issues of this newsletter can be found on the FedCIRC website www.fedcirc.gov/docs.html

FedCIRC is sponsored by the Federal CIO Council and is operated by the General Services Administration/Federal Technology Service